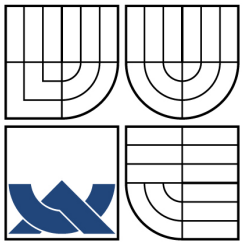
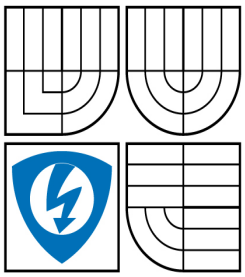


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV AUTOMATIZACE A MEŘICÍ TECHNIKY

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF CONTROL AND INSTRUMENTATION

ZABEZPEČOVACÍ SYSTÉM RD - MODUL VZDÁLENÉHO PŘÍSTUPU

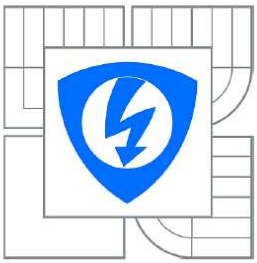
HOME SECURITY SYSTEM - REMOTE ACCESS MODULE

Bakalářská práce
BACHELOR'S THESIS

AUTOR PRÁCE — PETR ŠARDA
AUTHOR

VEDOUCÍ PRÁCE — Ing. PETR FIEDLER, Ph.D.
SUPERVISOR

BRNO 2010



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav automatizace a měřicí techniky

Bakalářská práce

bakalářský studijní obor
Automatizační a měřicí technika

Student:	Petr Šarda	***ID:***	109725
Ročník:	3	***Akademický rok:***	2009/2010

NÁZEV TÉMATU:

Zabezpečovací systém RD - modul vzdáleného přístupu

POKYNY PRO VYPRACOVÁNÍ:

Navrhněte koncepci připojení modulu vzdáleného přístupu (např. externí ethernetový modul), protokol, kterým bude modul komunikovat s ústřednou a způsob kterým bude modul vizualizovat stav ústředny. Realizujte SW zajišťující vizualizaci stavů simulované ústředny s využitím web serveru na zvolené HW platformě.

DOPORUČENÁ LITERATURA:

ČSN, uživatelské a instalační manuály zabezpečovacích ústředen

Termín zadání:	8.2.2010	***Termín odevzdání:***	31.5.2010

Vedoucí práce: Ing. Petr Fiedler, Ph.D.

prof. Ing. Pavel Jura, CSc.
Předseda oborové rady

ABSTRAKT V ČESKÉM JAZYCE + KLÍČOVÁ SLOVA

ABSTRAKT:

Práce se zabývá návrhem modulu vzdáleného přístupu pro Elektrické zabezpečovací systémy(EZS). Při návrhu se vychází z platných norem, které se vztahují na tvorbu Elektrických zabezpečovacích systémů. Obsahuje návrh propojení modulu vzdáleného přístupu s ústřednou, která řídí EZS. Dále je navržen komunikační protokol jak pro komunikaci s ústřednou, tak pro komunikaci modulu s uživatelem. Posledním krokem je návrh webového rozhraní, které je dále prakticky realizováno na vhodně zvoleném vývojovém prostředku.

KLÍČOVÁ SLOVA:

Elektrický zabezpečovací systém, Modul vzdáleného přístupu, propojení,Komunikační protokol, Signalizace, Webové rozhraní.

ABSTRAKT V ANGLICKÉM JAZYCE + KLÍČOVÁ SLOVA

ABSTRACT:

This thesis deals with remote access module for electric security systems (ESS). The design is based on valid standards that apply to a production of electric security system.
It includes a design of module connection to the central that controls the module. There is also a communication protocol for connection with the central and with the user. The last step is development of web interface, which is realized on the selected development kit.

KEYWORDS:

Electric security system, Remote Access module, Connection, Communication protocols, Signaling, Web interface.

Bibliografická citace

Šarda, Petr. *Zabezpečovací systém RD – Modul vzdáleného přístupu*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2010. 44s.

P r o h l á š e n í

Prohlašuji, že svou bakalářskou práci na téma “Zabezpečovací systém RD – modul vzdáleného přístupu“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.“

V Brně dne: Podpis:

P o ď ě k o v á n í

Děkuji tímto Ing. Petru Fiedlerovi, Ph.D. za cenné připomínky a rady při vypracování bakalářské práce.

V Brně dne : Podpis:

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

1. ÚVOD

Úkolem této práce je navržení externího modulu vzdáleného přístupu. Jedná se tedy o modul umožňující uživateli elektronického zabezpečovacího systému přístup do systému a provádění určitých změn, jako je nastavování například střežení určité oblasti. Úkolem je provést kompletní návrh vizualizace stavu ústředny na modulu, aplikovat požadavky na propojení modulu jak s ústřednou, tak do sítě, ze které bude mít možnost ho obsluhovat uživatel. Druhou částí úkolu je vytvořit funkční rozhraní pro ovládání modulu, kde bude navržený modul nahrazen odpovídajícím vývojovým hardwarem.

Ještě před samotným srovnáváním požadavků na zabezpečovací systémy a jejich srovnáváním by bylo vhodné si přiblížit co to vlastně zabezpečovací systém je. O co se jedná je přibližně jasné již ze samotného názvu. Jde většinou o elektricky řízené systémy, sloužící k ochraně majetku. Jsou používány jak na fázi zabezpečení velkých firem, cenností, tak čím dál tím více i pro ochranu osobního majetku, jako jsou rodinné byty a domy. Samozřejmostí je, že se tyto systémy pro různá využití liší jak v cenových relacích tak i ve složitosti provedení. Základní fáze je ale stejná a jde o to, že systém vyhodnocuje stav daných signálů a při jejich přerušení spustí alarm.

Simulační část se pokusím provést co nejsnazším způsobem tak, aby bylo dané webové rozhraní co nejlépe ovladatelné pro uživatele a jeho ovládání bylo jednoduché a přitom splňovalo základní parametry, které webové rozhraní splňovat má a které splňuje u běžně používaných modulů, které jsou v praxi používány u zabezpečovacích firem.

2. VŠEOBECNÉ POŽADAVKY NA ELEKTRICKÉ ZABEZPEČOVACÍ SYSTÉMY

Všeobecné požadavky stanovuje norma 50131: Část 1, která upřesňuje základní parametry, které mají splňovat jednotlivé části EZS. Tato kapitola se bude věnovat podrobnému rozebrání této normy. Tato norma určuje požadavky na elektrické zabezpečovací systémy jak se specifickým, tak nespecifickým vedením. Udává i požadavky na bezdrátové spojení. Tyto požadavky se týkají pouze EZS, které jsou použitelné pro vnitřní použití, nejsou směrodatné pro venkovní zabezpečovací systémy. Pravidla se dají aplikovat na komponenty venkovní ochrany, které jsou umístěny uvnitř budovy, jako jsou např. pomocná signalizační zařízení. Důležitým ustanovením této normy je to, že udává, že provoz EZS nesmí být narušen provozem jiného signálu[1] . Norma také udává různé požadavky pro různé prostředí. Popisuje tak prostředí ve kterém je předpoklad, že bude komponent EZS provádět svou práci. Jak již bylo také zmíněno rozdělujeme čtyři vlivy prostředí. Tyto podmínky jsou určeny všeobecně a proto je také vydáván doplněk A, který upřesňuje vlivy prostředí v národním měřítku[1].

Tato norma je všeobecnou evropskou normou. Ve svém těle obsahuje odkazy na různé publikace zabývající se EZS[1].

2.1 ATRIBUTY ZABEZPEČOVACÍHO SYSTÉMU

Každý EZS musí poskytovat možnosti pro detekci narušitelů, pro zpracování informací a pro ohlášení poplachů a dále prostředky pro provoz EZS[1]. Nejdůležitější atributy zabezpečovacího systému jsou shrnuty níže[1].

2.1.1 Funkčnost

Norma stanovuje každému EZS nějaký minimální rozsah funkcí, které musí systém umět splňovat. Není však podmínkou, že by systém nemohl mít více funkcí,

než je minimální rozsah zadaný normou. Dodatkové funkce však musí fungovat tak, aby nijak neomezovali a ani neohrožovali chod základních funkcí. Všechna EZS musí obsahovat následující funkce[1]:

- **Detekce** – Umožňuje rozeznání vniknutí nebo pokusu o něj do chráněné oblasti
- **Obslužná funkce**
- **Vyhodnocovací funkce** – Zpracovává informace z funkcí podobných jako je funkce detekční a musí být schopna reagovat na příkazy.
- **Výstupní funkce** – Jejím úkolem je poskytovat informace o činnosti EZS uživateli tohoto systému.
- **Funkce zabezpečení proti sabotáži**.

2.1.2 Spolehlivost

Spolehlivost systému může ovlivňovat několik možných atributů mezi které patří:

- **Vliv okolního prostředí**
- **Provozní spolehlivost**
- **Funkční spolehlivost**

Tyto atributy je třeba co nejlépe potlačit aby neměli vliv na práci systému a tím se zvyšovala jeho odolnost a funkčnost. Musíme tedy volit jednotlivé části systémů podle jejich vlastností do určitého prostředí. Vždy se musí vyjít ze zadání, kde má být EZS umístěn a za jakým účelem[1].

2.2 JEDNOTLIVÉ ČÁSTI ELEKTRICKÉHO ZABEZPEČOVACÍHO SYSTÉMU

Každý elektrický zabezpečovací systém musí být konstruován z několika částí, které přímo stanovuje daná norma. Části dané normou jsou následující:

- **Ústředna**
- **Jedno nebo více čidel**
- **Jedno nebo více signalizačních zařízení případně poplachových přenosových systémů**
- **Jedno nebo více napájecích zařízení, které mohou být kombinovány s jinými komponenty EZS nebo jsou samostatné**

Důležitým poznatkem je také to, že u jednotlivých částí EZS musí být stanovena bezpečnostní třída prostředí a musí být také řazeny podle daných stupňů zabezpečení.[1]

2.3 STUPNĚ ZABEZPEČENÍ

Rozlišujeme čtyři stupně zabezpečení, kde nejnižší požadavky jsou kladeny na nejnižší stupeň zabezpečení a nejvyšší požadavky na nejvyšší stupeň zabezpečení. Stupně zabezpečení jsou značeny čísli 1 až 4. Každý elektrický zabezpečovací systém musí mít stanoven stupeň zabezpečení. Ve stupni zabezpečení jsou shrnuty požadavky na:

- **Zabezpečení**
- **Přístupové úrovně**
- **Provozování**
- **Vyhodnocení**
- **Detekce**
- **Hlášení**
- **Napájení**
- **Zabezpečení proti sabotáži**
- **Monitorování propojení**

Je třeba také říci, že pokud je EZS dělen do subsystémů je možno, že každý subsystém obsahuje prvky jiného zabezpečovacího stupně. Nejnižší stupeň zabezpečení prvku, určuje zároveň stupeň zabezpečení celého subsystému. Nejnižší stupeň subsystému určuje stupeň zabezpečení celého EZS.[1]

Pokud předpokládáme, že jedna část EZS bude společná pro více EZS(například dva systémy se společnou ústřednou) musí být tyto části alespoň stejného stupně zabezpečení, nebo vyššího.[1]

Jednotlivé stupně zabezpečení jsou děleny následovně:

2.3.1 Stupeň 1: Nízké riziko

V tomto případě se počítá s tím, že možný narušitel má malou znalost elektrických zabezpečovacích systémů a tudíž je nižší riziko zdolání systémů[1].

2.3.2 Stupeň 2: Nízké a střední riziko

Předpokládá se, že možný narušitel disponuje alespoň základní znalostí zabezpečovacích systémů a je vybaven základními nástroji pro práci s nimi jako jsou např. přístroje měřící[1].

2.3.3 Stupeň 3: Střední a vysoké riziko

Definice je podobná jako u stupně zabezpečení č.2, předpokládá se ale, že narušitelé mají dobré znalosti z oblasti EZS a disponují veškerým vybavením pro práci s ním[1].

2.3.4 Stupeň 4: Vysoké riziko

Tento stupeň zabezpečení je využívám pouze v případě, že má ochrana nejvyšší prioritu. Předpoklady pro narušitele jsou totožné se stupněm ochrany č.3, ale předpokládá se, že narušitelé jsou schopni nahradit rozhodující části elektrického zabezpečovacího systému[1].

2.4 TŘÍDY PROSTŘEDÍ

Třídy prostředí se klasifikují z důvodu, aby činnost částí elektrických zabezpečovacích systémů měla správnou funkci. Rozlišujeme opět čtyři třídy, kde značení má vzestupnou tendenci, která označuje, že například prvky třídy IV můžeme použít i v aplikacích třídy III a níže. V samotných třídách jsou definovány např. požadavky na teplotu prostředí atd.[1]. Základní dělení tříd prostředí je následující:

- **Třída I - Prostředí vnitřní**
- **Třída II – Prostředí vnitřní všeobecné**
- **Třída III – Prostředí venkovní chráněné**
- **Třída IV – Prostředí venkovní všeobecné**

2.5 FUNKČNÍ POŽADAVKY

Jedná se o základní vlastnosti EZS, které jsou třeba k jejich správné funkčnosti. [1]

2.5.1 Detekce narušitelů a rozeznávání poruch

Toto je nezbytná funkce pro provoz jakéhokoliv EZS. EZS může samozřejmě obsahovat i detekci jiných parametrů, které ale svou detekcí nesmějí nijak narušovat práci detekce narušitelů, rozeznávání poruch a sabotáže. Tato detekce spočívá na sledování signálu. Pokud je signál přerušen je vyhodnocován jako pokus o vniknutí narušitele. Problém nastává v případě, kdy signálem sledujeme jak narušitele tak např. i sabotáž. Z logiky věci vyplívá, že z důvodu rozlišení o jakou část přerušení se jedná musíme zaručit, že signály od sebe budou odlišné[1]. Jednotlivé detekce si probereme podrobněji:

2.5.1.1 Detekce narušení

K této detekci jsou využívána čidla, které mají přesné určení pro dané prostředí ve kterém mají být použity. Možné typy snímacích čidel, jejich provedení a technologie:

- **Mikrovlná nebo ultrazvuková čidla**
- **Spínače pracující na magnetickém nebo mechanickém principu**
- **Čidla pohybu nebo čidla vibrační**
- **Pomocí akustické signalizace**
- **Optickým indikátorem na čidle**

2.5.1.2 Rozeznávání poruch

Nároky na rozeznávání poruch jsou opět dány stupněm zabezpečení do kterého spadá EZS. V každém případě musí být ale zajištěna indikace těchto poruch:

- **Všeobecná porucha**
- **Porucha základního napájecího zdroje**
- **Porucha náhradního napájecího zdroje**
- **Porucha přenosného poplachového systému(pokud je použit)**

Opět platí, jako v předešlém případě, že ostatní typy poruch mohou být také měřeny, pokud nijak neovlivňují funkci měření těchto čtyř základních poruch.[1]

2.5.2 Úroveň přístupu

Každý EZS musí být navržen tak aby umožňoval uživateli co nejednoduší a bezchybný přístup. Opět rozeznáváme několik druhů přístupů:

- **Úroveň 1 - Přístup pro každou osobu**
- **Úroveň 2 - Přístup pro každého uživatele**
- **Úroveň 3 - Přístup pro servisní pracovníky**
- **Úroveň 4 - Přístup pro výrobce**

Důležitou vlastností EZS je, že do úrovně č. 3 a 4. může být přístup proveden pouze pokud dá uživatel na úrovni č.2 souhlas[1]. Přihlášení do úrovní č.1,2,3, může být provedeno i dálkově za splnění daných zabezpečovacích podmínek.

2.5.3 Oprávnění

Oprávnění omezují přístupy do jednotlivých přístupů zabezpečení. Je tak činěno z důvodu, aby do systému nemohl zasahovat každý člen. Mohou do něj zasahovat pouze jedinci se speciálními přístupovými kódy. Veškeré oprávnění na EZS má jeho majitel, který může jednotlivá oprávnění rozdělovat mezi další subjekty. Jednotlivé základní přístupová oprávnění jsou shrnuty v tabulce č.1[1]:

Funkce/ovládání	Úroveň přístupu			
	1	2	*3	*4
Stav střežení		P	P	
Stav klidu		P	P	
Nulování ústředny		P	P	
Prověřování funkcí EZS (test)		P	P	
Zaprotokolování událostí		P	P	
Blokování/odpojení		P	P	
Přidání/změna kódu oprávnění		**P	**P	**P
Přidání/změna specifických dat			P	
Změna/náhrada základního programu				P

Tabulka č.1 – Tabulka jednotlivých oprávnění přístupů [1]

Označení P znamená povoleno, zašrafované body jsou zakázány. P s dvěma hvězdičkami jsou kódy na úrovni uživatelů s jednou tečkou mohou být využity pouze v případě že jsou nejdříve povoleny na úrovni zabezpečení č. 2.

2.5.4 Nastavování stavu střežení a stavu klidu

Stejně jako v předchozím případech je nutno aby pro zadání stavu klidu nebo stavu střežení byla udělena potřebná přístupová práva. Také je třeba opět dokázat zabezpečit aby uživatel mohl přepínat mezi stavy s co nejmenším zásahem do systému.[1]

2.5.4.1 Stav střežení

Stav střežení může být u EZS zadán pouze v případě, že všechny jeho komponenty jsou v normálním stavu. Je třeba také nějak zajistit aby EZS dal uživateli na vědomí, že je přepnuto do stavu střežení, tato indikace má podle normy uvedenou dobu trvání 180 sekund. Podmínkou pro uvedení čidla do stavu střežení je také to, že jsou všechna čidla EZS stabilizována. Pokud se nacházíme ve stavu střežení je třeba ošetřit příchod a odchod do střežené oblasti. K tomuto účelu slouží přístupová a odchodová cesta. Možným řešením je také to, že si dokáže systém sám indikovat zda se jedná o příchod nebo odchod.[1]

2.5.4.2 Stav klidu

Stejně jako v předchozím příkladě je nutno uvažovat, že stavu klidu lze dosáhnout pouze povolenou cestou, ke které má právo pouze oprávněný uživatel. Pokud je třeba před změnou stavu vstoupit do střežené oblasti, musí být toto konání povoleno již výše zmíněnou přístupovou cestou. Přístupová cesta vlastně označuje pojem, kdy jsou odpojeny čidla, která jsou na cestě k hlavnímu zařízení, kde se dá stav střežení přepnout do stavu klidu. Ostatní čidla (mimo přístupovou cestu) jsou stále v provozu až do ukončení přepnutí stavu. Povolená doba, za kterou je stav klidu nastaven je 45 sekund. Ukončení klidového stavu musí být signalizováno minimálně 30 sekund. [1]. Pokud za tuto dobu není nastavování stavu ukončeno musí být spuštěn poplachový systém. Pokud je užívána přenosná část EZS nesmí být poplachová část spuštěna dříve než po 30 sekundách od indikace. [1]

2.5.5 Ochrana proti sabotáži

Jedná se o další důležitou funkční vlastnost EZS. Samotná ochrana sabotáže spočívá v tom, že jednotlivé prvky EZS, musí být vybaveny tak, aby bylo co nejnesnadnější se dostat do vnitřních struktur a nastavení jednotlivých činností komponentů. Samotnou ochranu proti sabotáži ovlivňuje umístění komponentů(vně nebo uvnitř střeženého systému) a také ji ovlivňují požadavky na EZS. Všechny

nastavovací části musí být umístěny uvnitř krytů komponentů EZS. Tyto kryty musí být natolik odolné, aby nebylo možno je násilím otevřít aniž by to bylo vizuálně viditelné. Stejně tak musí být robustně zabezpečeny např. prvky ústředny.[1]

2.5.6 Další funkční požadavky

Předchozí části pouze ve zkratce ukázali a shrnuly některé požadavky na funkční požadavky EZS. Nejde ale samozřejmě o všechny funkční požadavky se kterými je třeba v rámci normy pracovat. Kvůli jejich objemnosti jsem se rozhodl podrobně uvést pouze některé, z řady dalších požadavků, které norma stanovuje. V mnohých případech požadavky, které tyto části udávají vyplývají již z jejich názvu[1]. Dalšími funkčními požadavky jsou:

- **Kompatibilita** – Jak je patrno už ze samotného názvu, jedná se o to, že jednotlivé prvky použité v EZS, musí být mezi sebou navzájem schopny spolupracovat[1].
- **Operace blokování** – Tato možnost umožňuje, že některé používané funkce EZS mohou být samotným systémem v průběhu činnosti pozastaveny nebo jejich spuštění může být přímo systémem zakázáno. Práva pro tuto činnost mají pouze uživatelé úrovně č.2. Důležité je také to, že pokud je nějaká činnost blokovaná po přepnutí do klidového stavu musí být všechna blokování zrušena.[1]
- **Operace odpojení (izolace)** – Zjednodušeně se dá říci, že se jedná o něco podobného jako je Operace blokování, akorát s tím rozdílem, že zde jsou jednotlivé funkce přímo odpojovány v režimu střežení samotným EZS. Přístup k těmto funkcím je dělen podle různých stupňů EZS. [1]
- **Vyhodnocení** – Vyhodnocení signálů nebo zpráv má být závislé na stavu EZS a typu signálu nebo zprávy.[1] Rozlišujeme následující typy možných zpráv a signálů:
  - **Poplachové signály nebo zprávy**
  - **Signály sabotáže**
  - **Poruchové signály**
- **Hlášení –** Jednotlivé stavy EZS jsou hlášeny podle toho v jakém aktuální stavu se zrovna EZS nachází. Hlášení může být provedeno jak pomocí signalizačního akustického zařízení, tak je také možnost toto hlášení provést jako vzdálený přenos. Pro dobu, jakou mají signály hlášení trvat jsou určeny mezinárodní nebo národní směrnice. Vždy jsou národní směrnice nadřazeny mezinárodním, protože mívají přísnější požadavky. [1]

- **Monitorování záměny –** EZS je nastaven, aby detekoval jednotlivé zařízení systému. Tato zařízení jsou pevně dána a vysílají specifický signál. Při záměně zařízení, musí být tato informace podána. V případě, že se tak stane v klidovém režimu je vyslán signál poruchy, v případě, že je tomu tak v režimu střežení, jedná se o signál sabotáže. Norma také určuje v jakých časových hodnotách musí být záměna detekována, např. pro stupeň zabezpečení č.2 je tato hodnota 60 sekund. Se zvyšujícím stupněm se požadavek na rychlost zvyšuje. [1]
- **Vyhodnocení –** Signály poplachu, poruchy nebo sabotáže, musí být rozeznány do 10 sekund. [1]

2.6 DŮSLEDKY NORMY NA NÁVRH MODULU VZDÁLENÉHO PŘÍSTUPU

Mým úkolem jak je uvedeno v úvodu je provést návrh modulu vzdáleného přístupu, který bude splňovat právě vlastnosti této normy. V mém případě budu navrhovat modul, který bude vyhovovat požadavkům první až druhého stupně zabezpečení a bude také vyhovovat stejným třídám prostředí, tedy třídám I a II. V případě, kdy budeme chtít použít ve vyšších stupních zabezpečení, bude to možno učinit, ale pouze ve chvíli, kdy to bude technicky možné a bude tato možnost vyhovovat nárokům daného EZS. Co se týče úrovní přístupu, bude modul navrhován na úroveň přístupu č.1, tedy přístup bude mít každá osoba.

3. PŘIPOJENÍ PERIFÉRIÍ K EZS

Velice záleží na možném typu ústředny ke které jsou jednotlivé periférie připojovány. Existuje několik standardů jak je možno periférie připojovat. Jedním z nich je tradiční použití drátových prostředků. Tento typ propojování je hojně využíván v případě propojování komponent např. uvnitř domu, kde slouží k propojení s ústřednou. Další možností je např. bezdrátové propojení, které je užíváno u venkovních komponentů. Jejich funkčnost spočívá ve vysílání signálu na ústřednu, která jej dále zpracovává. Pro vzájemné propojení jsou stanovena určitá pravidla, která si shrneme níže. [1]

3.1 PROPOJENÍ

Základním požadavkem na propojení je to, že má co nejvýhodněji spojovat jednotlivé prvky, které spolu pomocí tohoto propojení bezchybně komunikují. Norma přímo udává, že propojení může být realizováno následovně:

- **Specifické pevné vedení**
- **Nespecifické pevní vedení**
- **Bezdrátové propojení**

U každého propojení musí být při realizaci počítáno s tím, že je požadavek na to, aby bylo veškeré propojení monitorováno a kontrolovalo, že komunikace mezi jednotlivými komponenty probíhá bezchybně. Pro samotné zjištění funkčnosti komunikace se využívá tzv. periodická komunikace. Z důvodu aby bylo zajištěno, že jeden prvek EZS nepůjde nahradit jiným prvkem za běhu, tedy, že narušitel nahradí stávající signál jiným je třeba zajistit monitorování. [1]

3.1.1 Periodická komunikace mezi komponenty

Norma přesně udává v jakých časových intervalech musí být komunikace zajišťována. Časové intervaly jsou shrnuty v tabulce č.2:

Četnost komunikací	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
V průběhu nastavování stavu střežení	Nepovinné	Povinné	Povinné	Povinné
Četnost komunikací	4	2	1	15

Tabulka č.2 – Periodická komunikace mezi komponenty[1]

Z tabulky je opět patrno, že velký vliv na periodickou komunikaci mezi komponenty má zvolený stupeň zabezpečení EZS. Také je z ní patrno, že pouze u prvního stupně se nemusí navazovat komunikace při nastavování změny stavu z klidového do stavu střežení. Systém vyhodnocuje signály mezi komponenty v daných časových intervalech a v případě, že signál není navázán systém přejde do stavu, kdy vysílá poruchový signál. Toto se děje pokud je systém v klidovém stavu, pokud se nachází ve stavu střežení a periodicky komunikuje a není spojení navázáno počítá se s možnou sabotáží systému a je vydán signál sabotáže. Je potřeba také říci, že části EZS, které mají pevné umístění a nedá se s nimi manipulovat, tedy např. ústředna EZS musí nutně požadavky na periodickou komunikaci splňovat. Není tomu tak už u částí EZS, které jsou přenositelné. Tyto části nemusí umět periodicky komunikovat a ani daná norma jim tuto vlastnost neurčuje.[1]

Pod pojmem periodická komunikace si můžeme představit průběh nějakého (téměř libovolného) detekovaného signálu. Takovým typem signálu který je pro tento účel použitelný je elektrický proud, který prochází přes nějaký spínač, který jej spíná v časových intervalech nebo pomocí magnetického pole. Tímto spínáním je zaručena detekce daného komponentu EZS. Pokud se jedná o EZS s ústřednou je tento problém vyřešen tak, že všechny prvky musí komunikovat s ústřednou, která jejich přítomnost vyhodnocuje, dá se však také provést zapojení EZS, které ústřednu vůbec neobsahuje (bez zapojení ústředny). V tomto případě spolu komunikují pouze nějaké

části EZS nebo všechny části v případě, kdy je použito ústředny komunikují všechny zbylé části EZS s ústřednou. [1]

3.1.2 Monitorování

Monitorování je důležitou součástí, které se používá zároveň a na úrovni se samotnou komunikací. Rozeznáváme několik druhů monitorování a to monitorování pro:

- **Propojení**
- **Záměny**
- **Intervalů [1]**

3.1.2.1Monitorování Propojení

Dá se říci, že toto monitorování probíhá pouze z důvodu, že pomocí něho kontrolujeme zda vůbec může dojít k navázání spojení a zda komponenty EZS mohou být navzájem spojeny. Stejně jako ve většině předešlých případů jsou přesně stanoveny doby, ve kterých musí být ověřeno, že je možno uskutečnit propojení mezi dvěma zařízeními. Jednotlivé časové požadavky se také liší podle toho o který zabezpečovací stupeň se jedná. V případě prvního a druhého stupně musí být propojení zjištěno v intervalu 30 až 60 sekund. Pro třetí a čtvrtý stupeň je to 10 až 20 sekund. Při nenavázání propojení v daném intervalu se obdobně jako u periodické komunikace definují dva rozdílné signály a to pro stav střežení a klidu, které jsou naprosto stejné. V případě klidu jde o vygenerování signálu poruchy v případě střežení jde o signál sabotáže.[1]

Zajímavostí může být to, že doby zkoušení navázání komunikace jsou pevně stanoveny na výše zmíněných 60 a 20 sekund, ale propojení musí být dosaženo za polovinu této doby. K propojení nemusí dojít z několika důvodů jako jsou např. důvody kdy dojde ve velkém propojení k interferenci s jinými aplikacemi nebo například z důvodu poškození samotného vedení. [1]

K samotnému propojení jsou používány následující možnosti:

- **Systém se specifickým trvalým vedením**
- **Systém se společným trvalým vedením**
- **Bezdrátové vedení**

V jednotlivých systémech mají chybové hlášení různé důvody a vyjadřují různé věci. V případě systému se specifickým trvalým vedením se při špatné detekci signálu jedná o možnou chybu propojení nebo může být problémem chyba vzniklá uvnitř komponentu se kterým se snažíme komunikovat. V případě systému se společným trvalým vedením jsme schopni určit problémy stejné jako v případě předchozího systému se specifickým trvalým vedením, ale navíc jsme schopni monitorovat zda například nedochází k narušení spojení z jiných aplikací. Obdobně je to i při bezdrátovém připojení, ale pomocí radiového kanálu můžeme monitorovat jednotlivé části, které by mohli samotný přenos narušit. [1]

3.1.2.2 Monitorování záměny

Spočívá v zjišťování možné náhrady signálu nebo zprávy z jednotlivých komponent EZS zpracovávaných ústřednou. Opět dochází k dvěma možnostem jako u většiny předcházejících případů, které se projevují ve chvíli, kdy je zaznamenána detekce jiného zařízení, v případě klidového stavu se jedná o vyslání poruchové zprávy v případě stření jde jako v předchozích případech a signál sabotáže. [1]

Norma určená pro tento typ monitorování udává stejně jako v přecházejícím příkladě i časové požadavky, za které musí být záměna detekována.[1]

Časové požadavky se opět liší podle stupně zabezpečení EZS. Se vzrůstajícím stupněm zabezpečení je doba detekce stále kratší. Pro čtvrtý stupeň je hodnota stanovena na 10 sekund, pro třetí stupeň zabezpečení na 20 sekund a pro druhý stupeň na 60 sekund. Co se týče prvního stupně zabezpečení není přesně daná časová

hodnota detekce, naopak norma dává výrobcům tu možnost že v tomto případě nemusí detekci záměny signálu brát vůbec v potaz a celý systém může fungovat bez ní. Z tohoto poznatku logicky vyplývá,že nebudu tento systém schopen detekovat, že se k němu snaží připojit jiné zařízení, je ale nutno také říci, že v případech uvažovaného prvního stupně zabezpečení není toto až takovým problémem a nepředpokládá se, že by někdo chtěl tento systém narušovat. Následující tabulka shrnuje požadavky na monitorování podle dané normy pro všechny stupně zabezpečení.[1]

Požadavky na monitorování	Stupeň 1	Stupeň 2 [s]	Stupeň 3 [s]	Stupeň 4 [s]
Náhrada komponentů EZS	Op	60	30	10
Náhrada signálů/zpráv	Op	60	30	10

Tabulka č.3 – Časové intervaly pro monitorování záměny [1]

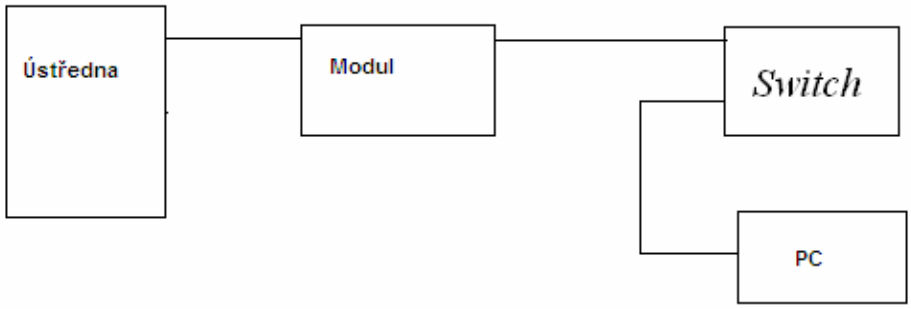
4. NÁVRH MODULU VZDÁLENÉHO PŘÍSTUPU

Dá se říci, že se jedná o komunikační modul, který slouží k tomu aby byl instalován přímým připojením k samotné ústředně. Pomocí modulu by mělo být možno měnit jednotlivé vlastnosti v nastavení EZS jako je například nastavování střežení pro určité oblasti daného EZS. Uživatel by měl být schopen EZS ovládat i z jiných míst, než je místo ve kterém je umístěn samotný EZS.

4.1 NÁVRH PROPOJENÍ

Nároky na propojení stanovuje norma ČSN. Všechny požadavky na propojení jsou rozebrány blíže v kapitole č.3.

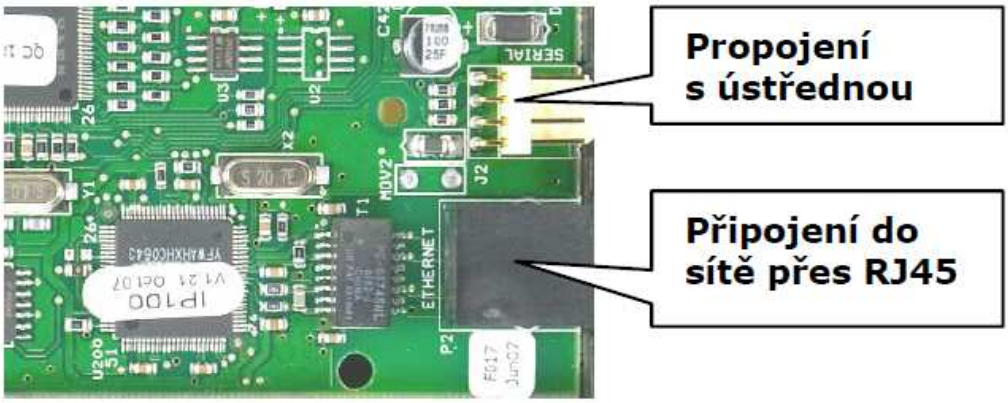
Pokud se budeme zabývat samotným síťovým propojením komunikačního modulu je třeba si stanovit pro jaké prostředí bude modul používán. Jak bylo již řečeno výše, modul bude navrhován pro třídu prostředí I a II, tedy pro vnitřní použití. V mém případě bude modul ovládán pomocí webového rozhraní. To znamená, že na modul by se mělo být možno připojit z libovolného místa, které je připojitelné do sítě Internetu, tímto zároveň vyplývá požadavek na to, že domácí síť musí mít přidělenu veřejnou IP adresu. Zároveň by se mělo být možno připojit i z lokální sítě, tedy pro obsluhu mít možnost využít i domácího PC. Pro tyto potřeby je vhodné užití síťových prostředků SWITCH nebo HUB.[1] Příklad takového propojení je zobrazen na **Obrázku č.1**. Další možností je přímé připojení pomocí křížového kabelu, které se ale nedoporučuje, protože spolehlivost tohoto připojení je značně nižší než spolehlivost připojení využívajícího síťové prostředky. Pro toto připojení by bylo využito tedy Ethernetu a připojení by bylo fyzicky provedeno pomocí konektoru RJ45.



Obrázek č.1 – Doporučené propojení modulu s PC v lokální síti

Pro komunikaci se samotnou ústřednou EZS je třeba stanovit si pravidla i pro toto připojení. Já jsem se u svého návrhu rozhodl pro použití asi nejrozšířenější varianty a to, že pro komunikaci s ústřednou užiji spojení sériovou linkou. Toto spojení volím z prostého důvodu a tím je, že pokud chceme vytvořit vlastní komunikační protokol, který bude řídit vzájemnou komunikaci mezi modulem, ústřednou a síťovým prostředím, tak je třeba zvolit takové propojení, aby bylo možno tento vlastní komunikační protokol realizovat. Nejednoduší možností je právě sériová linka, protože například na průmyslových sběrnicích jako je I2C by se nám zřejmě vlastní protokol definoval velice špatně. Modul bude tedy propojen pomocí sériové linky s ústřednou, což klade samozřejmý požadavek i na ústřednu, která musí být vybavena portem pro připojení sériové linky.

Ukázka modulu s podobným propojením je zobrazena na následujícím obrázku:



Obrázek č.2 – Modul vzdáleného přístupu se sériovou linkou a RJ45[2]

V této části, zabývající se propojením modulu s ústřednou a webovým rozhraním je třeba se dle mého názoru také zmínit o napájení modulu. Napájecí napětí, které standardně moduly využívají je 12V. Možnost napájení se dá řešit dvěmi možnými způsoby. Prvním z nich je možnost, že by měl modul vlastní napájecí zdroj. Druhou možnosti je napájení přímo od ústředny přes připojený konektor. První možnost má výhodu v tom, že máme nezávislí zdroj, takže v případě poruchy napájení ústředny modul stále poběží. Osobně mi přijde tato možnost mnohem lepší z toho důvodu, že pokud dojde k poruše na napájení ústředny, modul je napájen stále a je možno se na něj stále přihlásit a ošetřit stav tak, aby modul na webovém rozhraní signalizoval, že informace od stavu EZS od ústředny nelze získat a tedy se vyskytl problém mezi komunikací ústředny a modulu vzdáleného přístupu jako je např. právě výpadek napájení ústředny. Pro svůj modul bych přesto volil napájení pomocí připojení na sériovou linku z důvodu, že je to cenově výhodnější varianta a také se by se mohl eventuelně vyskytnout problém s napájením, např. nemožnost zapojení zdroje do sítě, nebo jeho nemožnost umístění v blízkosti samotného modulu. Tento problém s napájením přímo od ústředny odpadá.

Pro návrh mého modulu bylo tedy navrženo následující propojení, které je shrnuto v následující tabulce:

Tabulka návrhu propojení	
Propojení odkud - kam	Použité síťové rozhraní
Ústředna - Modul	Sériová linka
Modul - PC	Ethernet/Internet

Tabulka č.4 – Konečný návrh propojení navrhovaného modulu

Základní propojení by mělo být stejné jako je zobrazeno na **Obrázku č.1**

4.2 KOMUNIKAČNÍ PROTOKOL

Nejdříve je vhodné říci, co to vlastně komunikační protokol je. Podle dané definice se jedné o pravidla určující nějaký standart podle kterého probíhá elektronická komunikace a také přenos dat mezi dvěma koncovými body. V našem případě se tedy navrhovaný komunikační protokol bude vztahovat na komunikaci a přenosu dat mezi modulem vzdáleného přístupu a ústřednou elektrického zabezpečovacího systému. Základem je tedy třeba si definovat informace, které budou ve vzájemné komunikaci přenášeny od ústředny k modulu a které informace bude moci uživatel pomocí modulu měnit v nastavení ústředny.

4.2.1 Přenášené informace do modulu

Při použití mnou navrhovaného modulu bych rád umožnil , aby bylo možno použít co nejkompletnější možnost ovládání. Co se týče informací, které by měli být od ústředny poskytovány modulu, mělo by jít hlavně o informace týkající se aktuální stavu a nastavení celého EZS. Nutno je také se zmínit, že je vhodné EZS rozdělit na jednotlivé podsystémy, např. pokud má obytný dům garáž, tak můžeme rozdělit systém na oblast týkající se garáže a další oblast týkající se střežení rodinného domu. V tomto případě nám systém umožňuje nastavovat stavy systému (střežení a klid) zvlášť pro dům a garáž. To vlastně v praxi znamená, že pokud nejdeme do domu,

můžeme ho nechat střežený a vypnout zabezpečení pouze na garáži, do které se potřebujeme dostat. Informace o stavech těchto podsystémů by měli být rozhodně přenášeny po sériové lince do modulu vzdáleného přístupu, který by je dále měl vizualizovat uživateli na webové rozhraní. Uživatel by právě pomocí webového rozhraní měl být schopen toto nastavení systému ovlivnit. Pokud se týče toho, měl by být pomocí modulu schopen ovlivnit pouze stav z nestřeženého na střežený, opačná možnost je dle mého názoru naprosto zbytečná z důvodu, že zrušení střežení na dálku zřejmě nikdo chtít dělat nebude a také by to bylo krajně nevhodné z důvodu samotné bezpečnosti.

Další informace, které by měla poskytovat ústředna modulu a ten je zobrazovat uživateli by měli být následující:

- Stav záložního zdroje energie systému
- Stav jednotlivých čidel a prvků EZS, např. nepodařilo se navázat spojení s daným prostředkem (např. klávesnice)
- Stav EZS, je-li v režimu střežení nebo klidu.
- Informace o jednotlivých objektech (datum instalace, jejich typ)

Podle mnou zjištěných informace se jedná o základní stavy, které jsou předávány u jednotlivých firem zabývajících se výrobou komponent pro EZS a jejich instalací.

Můj modul by měl splňovat tedy následující požadavky a ještě bude předával informace pomocí modulu o tom zda je spuštěno alarmové hlášení, protože mi to přijde jako vhodné, aby byl uživatel při spuštění informován o tom, že se kupříkladu do jeho domu někdo pokoušel vloupat.

4.2.2 Co se dá pomocí modulu měnit na ústředně

Informace, které byli v předchozí kapitole popsány se týkají přenosu od ústředny do modulu, včetně již blíže popsaných subsystémů a jejich vizualizace na webové rozhraní. Právě pomocí zadání na tomto rozhraní by měl být modul schopen prostřednictvím ústředny měnit stavy těchto podsystémů (pouze přepínání do stavu

střežení např. z důvodu, že uživatel zapomněl objekt uvést do stavu střežení). U jednotlivých firem, je pomocí modulu vzdáleného přístupu umožňování komplexního nastavení celého systému EZS. To znamená, že můžeme nastavovat jména jednotlivých podsystémů, které části budou do podsystému zahrnuty (v tomto případě může jít o označení jednotlivých čidel nebo více sdružených čidel, většinou se vztahujících na nějaký daný prostor). Ve většině případů je pomocí modulu možno nastavovat i čas, který je na ústředně.

Co se týče samotné funkčnosti ovládání, nejdůležitější částí je ovládání jednotlivých systémů. Jak již bylo několikrát zmíněno, mělo by být možno změnit stav subsystému na střežení. Dále by mělo být možno ovládat, jednotlivé části podsystému. Tímto je myšleno např. možné odpojení nějaké čidla dané části systému. Jako příkladem může být opět střežení garáže, kde můžeme střežit např. jedním čidlem oblast před garáží a druhým čidlem oblast, která se týká vnitřního prostoru naší garáže. Ovládáním pomocí modulu můžeme tedy uskutečnit to, že odpojíme tu část před garáží a necháme střežit pouze část, která je v garáži. Jedná se vlastně o podobné řešení jako je řešení pomocí samotných podsystémů, ale ty jsou děleny ještě na menší jednotky, kterým se také říká střežící zóny.

Dále by mělo být možno u jednotlivých částí vypnout alarmové hlášení. Tato součást není u výrobců EZS využívána, ale v mém případě bude zahrnuta, protože mi tato možnost přijde docela vhodná z důvodu, že pokud bude alarm již spuštěn a informace zaslány, není třeba udržovat alarmový stav a může se opět přejít do stavu střežení.

4.2.3 Shrnutí pro komunikaci

Konečný návrh pro mnou navrhovaný modul vzdáleného přístupu je shrnut v následující tabulce :

Přenášená data	
Odkud - Kam	Data
Ústředna - Modul	Stav záložního zdroje energie systému
	Stav jednotlivých čidel a prvků, např. nepodařilo se navázat spojení
	Stav EZS
	Informace o jednotlivých objektech
Uživatel - Modul	Možnost nastavení IP adresy
	Změna stavu čidel
Modul - Uživatel	Stejné vlastnosti jako v případě přenosu Ústředna - Modul

Tabulka č.5 – Navržené vlastnosti komunikace mezi jednotlivými komponenty

4.3 SIGNALIZACE STAVU ÚSTŘEDNY A SYSTÉMU POMOCÍ MODULU VZDÁLENÉHO PŘÍSTUPU

Signalizaci prováděnou pomocí modulu bych rád rozdělil na dvě základní části. První signalizace by měla udávat stav spojení ústředny a samotného modulu. Tato signalizace by měla být prováděna pomocí skupiny LED diod. Mohla by to být skupina zelené a červené diody, kde zelená dioda by signalizovala, že propojení mezi oběma částmi proběhlo v pořádku a je navázáno. V případě rozsvícení červené diody bude signalizováno, že spojení mezi ústřednou a modulem není navázáno a tedy je potřeba blíže určitě problém, který se vyskytl a zajistit jeho odstranění. Tento problém by mohl být vypsán také na webové rozhraní, které by měl mít uživatel, jak již bylo několikrát zmíněno přístupno z jakéhokoliv PC, nebo jiného prostředku, který je připojitelný do sítě Internetu, nebo je v lokální síti a má přístup na modul, např. propojení na **Obrázek č.1**, kde je použito k propojení síťového komponenty Switch. Informace zobrazená na tomto rozhraní by měla blíže specifikovat chybu, která v navazování propojení vznikla.

Druhou částí, týkající se vizualizace je právě webové rozhraní. Jak bylo uvedeno výše, pomocí webového rozhraní bude možno obsluhovat ústřednu a také pomocí něj

budeme moci vidět aktuální stav ústředny. Budou na něm zobrazeny jednotlivé podsystémy, kde budou odlišnými způsoby zobrazovat stav, ve kterém se daný podsystém nachází. Dále bude také jiným způsobem signalizován stav, kdy bude spuštěno alarmové hlášení.. Jako příklad pro volbu vizualizace mi posloužilo rozhraní firmy Paradox na jejich komunikační modul IP100. Jednotlivé zobrazení stavů by tedy mohlo odpovídat následujícímu zobrazení, které je ukázáno na **Obrázek č.3**. Pro svůj modul bych rád využil podobně jednoduché signalizace, která by signalizovala jak stav kompletního systému, tak stav jednotlivých podsystémů.

Dále by se dalo také uvažovat o signalizaci pro jednotlivé části podsystémů. Nebylo by zde již uvedeno zda je ve stavu střežení nebo klidu (to se týká systému a podsystémů), ale určovalo by, zda je zařízení funkční a nebo zda v provozu není.

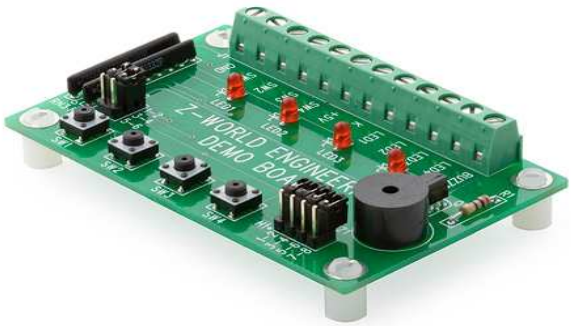
Obrázek č.3 – Příklad webového rozhraní[2]

5. SIMULACE OVLÁDÁNÍ POMOCÍ WEBOVÉHO ROZHRANÍ

Dalším úkolem řešené problematiky bylo určit jakým způsobem bude probíhat obsluha daného modulu pomocí webového rozhraní. Pro tento účel jsme zvolily možnost simulace tohoto rozhraní na vývojovém hardwarovém prostředku, který obsahuje procesor RABBIT 2000 a také tento hardwarový prostředek obsahuje možnost připojení k Ethernetu. Jedné se tedy o TCP/IP Development Kit. Jde sice o starší hardwarový prostředek, ale pro naše účely je plně postačující. Vývoj na prostředku je prováděn pomocí programovacího jazyka dodávaného výrobcem procesoru RABBIT a jedná se o jazyk C s nejrůznějšími úpravami pro správnou funkčnost na daném procesoru.

5.1 PROGRAMOVÁNÍ ÚSTŘEDNY

Pro správnou funkci obsluhy modulu přes webové rozhraní, bylo třeba provést několik úkolů. Prvním z těchto úkolů bylo nějakým způsobem naprogramovat ústřednu, aby bylo možno vůbec něco simulovat přes webové rozhraní a na něm také zobrazovat zda je nějaké čidlo v provozu či ne, nebo zda je systém ve stavu, kdy je sepnut alarm. V mém případě byla jako ústředna použita Z-World Engineering Demo Board, která je ukázána na následujícím obrázku.

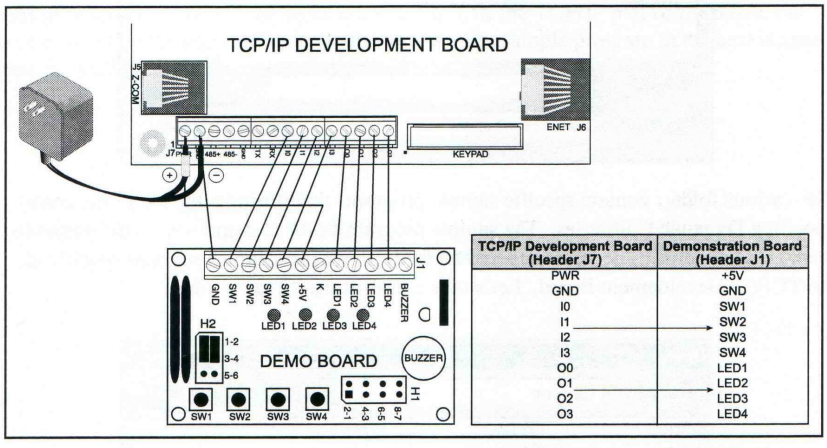


Obrázek č.4 – Hardware, na kterém probíhá simulace ústředny[3]

V mém případě, jsem se pokusil rozdělit signalizaci čidel na stav, kdy jsou čidla ve stavu zabezpečení, svítí diody a na případ, kdy zabezpečena nejsou, Jednotlivé snímače jsou rozděleny do dvou skupin a ty se dají rozdělit jako skupina, která zabezpečuje jedno prostředí např. Garáž (V mém případě se jedná o jednu diodu, která je spouštěna a vypínána daným tlačítkem). Jako další jsem se rozhodl jedním tlačítkem spustit zabezpečení domu, tedy dvě čidla (Daným spínačem provedeme sepnutí dvou diod, z nich jedno značí například čidlo vchodových dveří a druhé zadní vchod, stejným spínačem jsou také vypnuty).

Další věcí, kterou bude ústředna umožňovat je možnost spuštění alarmu. Alarm by měl být logicky spouštěn pouze v případě, kdy jsou čidla zabezpečená (ledky svítí). V mém případě, je toto uděláno pomocí spínače, který spouští alarm, podle stisků na jednotlivá čidla. Pro lepší vizualizaci je také nastaveno, že v případě sepnutí poplachu, všechny čidla, která jsou ve střežícím režimu, tedy diody, která svítí začnou blikat a alarm je také doprovázen akustickým signálem. Toto řešení je opravdu pouze simulační, ale jedná se asi o nejvhodnější způsob, jakým se dá tato činnost provést, protože nejsou k dispozici jednotlivá čidla a tedy nelze s nimi přímo pracovat, proto jsem se rozhodl pro toto řešení.

Všechny tyto části jsou vytvořeny pomocí Dynamic C na procesoru Rabbit, který je propojen s deskou, která slouží jako simulace ústředny. Samotné propojení je provedeno následujícím způsobem:



Obrázek č.5 – Propojení modelu ústředny s vývojovým hardwarem[4]

5.2 WEBOVÉ ROZHRANÍ

Po vytvoření obsluhy ústředny je třeba nastavit vytvořit příslušné webové rozhraní, jehož základem je vytvoření nějaké obslužné stránky. V mém případě půjde o velice jednoduchou stránku, která bude umožňovat uživateli ovládání jednotlivých čidel, které budou zobrazovány na vývojovém prostředku rozsvěcením jednotlivých příslušných LED diod. Jak již bylo zmíněno výše, půjde pouze o možnost zabezpečení čidel, která bude projevována tak, že budou diody rozsvěceny. Další vlastnosti, které bude rozhraní splňovat bude možnost detekování alarmového hlášení a také informace o celkovém nastavení systému EZS a důležitá je také možnost nastavení síťové adresy, podle které bude navazována komunikace s modulem. Tato funkce bude prováděna za pomoci samotného modulu vzdáleného přístupu.

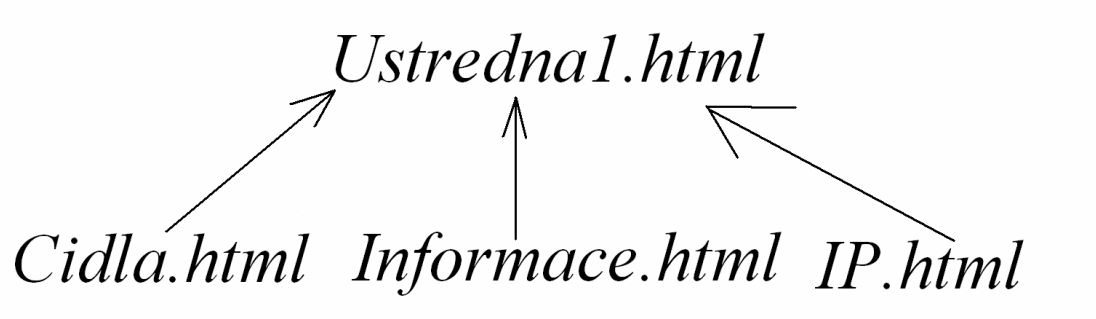
Samotné webové rozhraní bude tedy vytvořeno ze tří základních částí, které si dále podrobněji popíšeme. Půjde o část, která bude sledovat jednotlivá čidla a bude uživateli umožňovat v případě, že nějaké čidlo není v provozu toto čidlo uvést do režimu střežení a v případě kdy je sepnuto hlášení alarmu, bude umožněno pomocí modulu toto hlášení detekovat a následně vypnout.

Další část se bude zabývat jednotlivými informacemi, které se budou věnovat kompletnímu nastavení EZS. Bude mít dvě hlavní části. První částí bude informace o tom, která čidla jsou zastřežena a jako druhá poté informace, zda je energie pro napájení EZS brána z akumulátoru nebo nikoliv. Tyto standardní vlastnosti umožňují téměř všechny moduly vzdálených přístupů k EZS, které jsou komerčně vyráběny a také běžně používány.

Poslední částí bude možnost nastavení vlastní adresy IP uživatelem. Bude to uskutečněno tak, že budou podporovány pouze určité IP adresy v daném rozsahu.

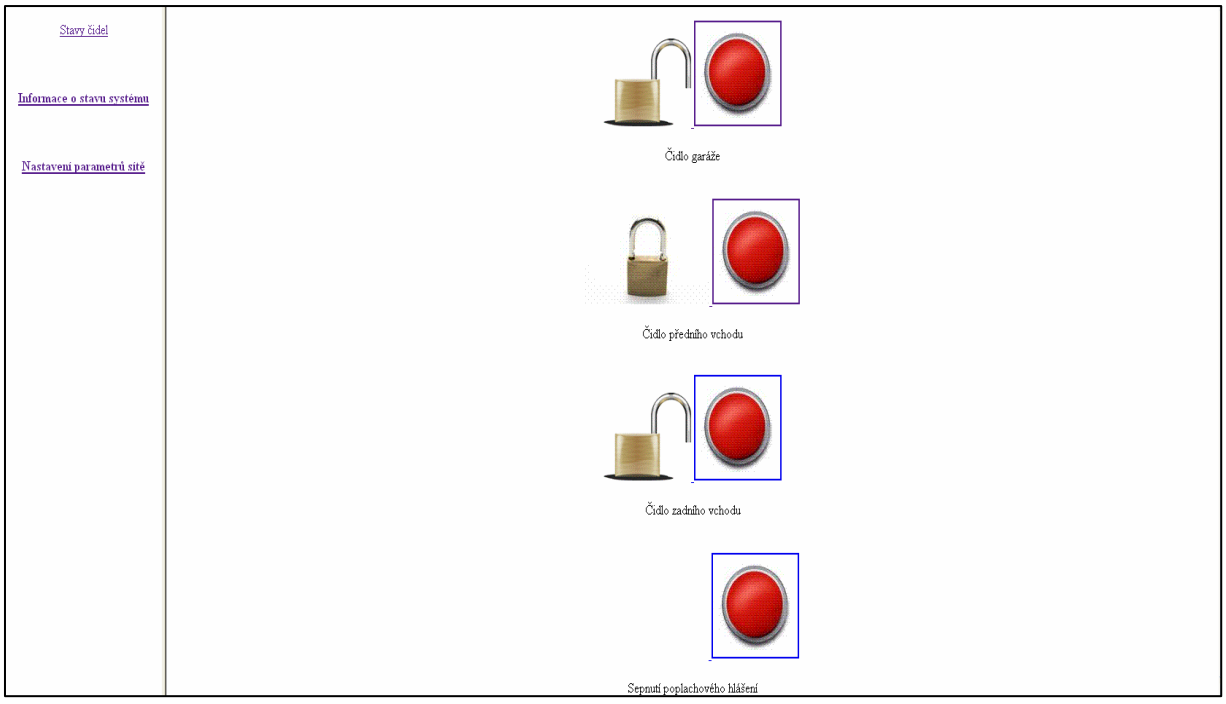
Z důvodu vytvoření webového rozhraní bylo třeba vytvořit webové stránky. Tyto stránky bylo tvořeny na základě jednotlivých informací, které měli být v různých částech zobrazovány. Jak je tedy patrno, byli vytvořeny tři základní stránky, které se zabývali jednotlivými, výše zmíněnými částmi. Zobrazována je pouze hlavní stránka, která je rozdělena na dvě části a to na část, která označuje MENU stránek a druhá část slouží pro zobrazování samotných stránek a informací, které jsou uživateli

poskytovány a zároveň také možností, které může uživatel v nastavení EZS pomocí modulu vzdáleného přístupu ovlivňovat. Základní rozvrstvení stánek, včetně jejich originálních názvů je vytvořeno v následujícím schématu.



Obrázek č.6 – Schéma závislosti vytvořených webových stránek

Všechny tyto části jsou zobrazovány v základní části týkající se textu. V levé straně je vždy zobrazen obsah, který umožňuje přepínaní mezi jednotlivými částmi ovládání a informačními částmi rozhraní, tedy mezi jednotlivými vytvořenými stránkami. Základní zobrazení webového rozhraní je ukázáno na následujícím obrázku.

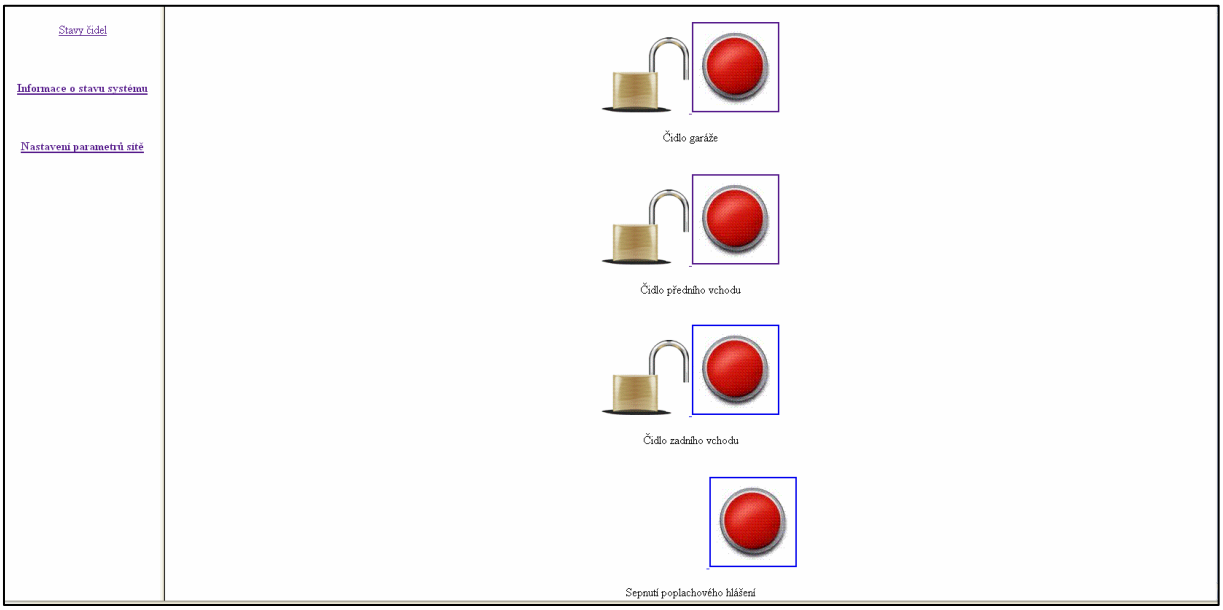


Obrázek č.7 – Základní zobrazení webového rozhraní

5.2.1 Ovládání a simulace jednotlivých čidel

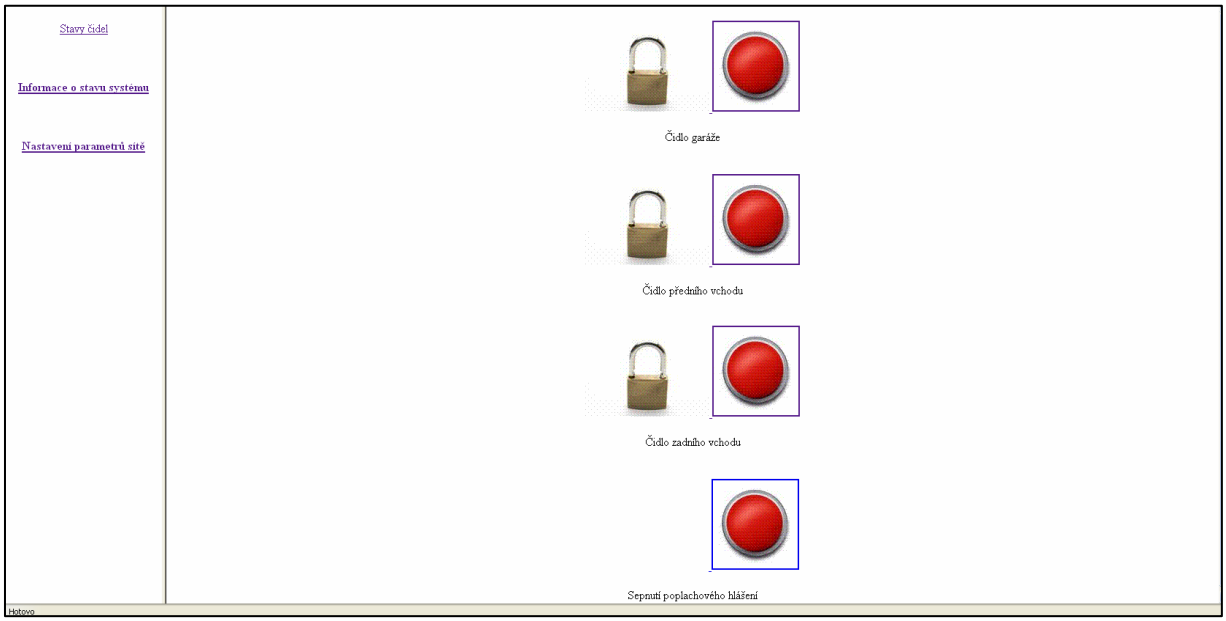
Jak již bylo několikrát zmíněno, základní funkcí této části je to, že zároveň simuluje stav jednotlivých čidel, které jsou v EZS zapojeny a také umožňuje uživateli provést zastření jednotlivých čidel, pokud tak není vykonáno již dříve. Tato možnost je běžnou součástí, která je používána u jednotlivých firem, zabývajících se výrobou EZS. Jak již bylo také zmíněno ve svém návrhu jsem se rozhodl přiřadit navíc možnost vypnutí alarmu pomocí modulu vzdáleného přístupu. Tato část se může jevit částečně jako zbytečná, ale dle mého názoru je vhodné ji zařadit z hlediska, že v případě, kdy je policie již informována není třeba udržovat nadále alarmové hlášení a tudíž neupozorňovat nějakým zbytečným způsobem samotného narušitele. Tato část není ale u standardních výrobců EZS používána.

Základním problém při návrhu této části bylo sjednocení možnosti zadání zastřežení čidla pomocí ústředny (V našem případě jde o Z-World Engineering Demo Board, která funkce ústředny simuluje) a také možnost zadání možnosti zastřežení pomocí modulu vzdáleného přístupu. Stejný problém byl i s vypínáním alarmového hlášení. Tato část byla nakonec provedena tak, že je možno provádět obě tyto možnosti společně, tak aby se nerušili. Dostat jednotlivá čidla do klidového stavu, lze pouze pomocí sepnutí z ústředny. Uživatel při spojení s modulem vzdáleného přístupu a výběru stránky zobrazují stav jednotlivých čidel, získává následují pohled na zabezpečení systému.



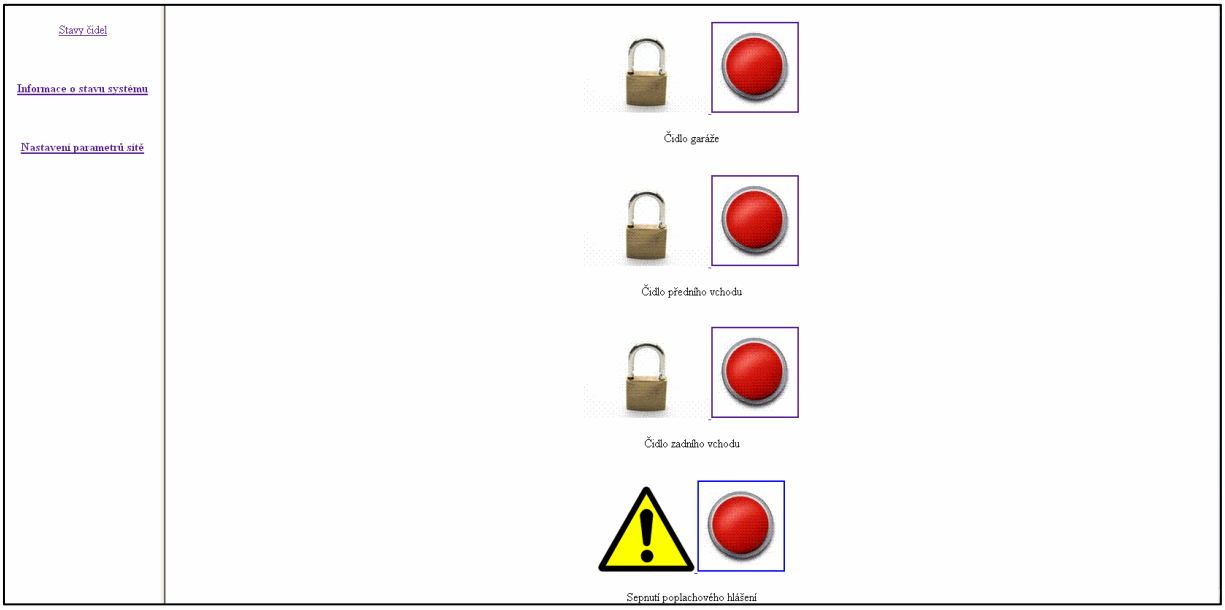
Obrázek č.8 – Část webového rozhraní signalizující stavy čidel

Jak je vidět, základní nastavení je provedeno tak, že jsou všechna zobrazená čidla znázorněno jako otevřená. Při aktualizaci stránky, je ale již zobrazeno přesné nastavení EZS, které je právě aktuální. Označení jako otevřený zámek logicky značí že čidlo není zabezpečeno v případě že čidlo zabezpečíme se toto označení mění na zamčený zámek. Změnu lze jak již bylo řečeno provést jak na základě nastavení na samotné ústředně, tak lze zabezpečení lze provést pomocí červeného tlačítka, které je umístěno vedle signalizací stavu čidel. Každé čidlo je navíc označeno popisem. V našem případě tedy máme tři čidla, jedno pro garáž, druhé pro přední vchod a třetí pro vchod zadní. Případ, kdy jsou všechna tři čidla zabezpečena je zobrazen na následujícím obrázku.



Obrázek č.9 – Vizualizace sepnutí čidel na webovém rozhraní

Část týkající se sepnutí alarmu je zobrazena v nejspodnější části stránky. V případě, kdy není alarm sepnut je zobrazeno pouze tlačítko, které alarm vypíná. Toto zobrazení je uskutečněno tak, že do funkce, která zobrazuje stavy je přidán prázdný bílý čtverec, který je brán jako signalizace v případě, kdy není spuštěn alarm. V případě, že je alarm spuštěn přecházíme se ve vizualizace webovým rozhraním do stavu, kdy je vedle příslušného červeného tlačítka provedena signalizace pomocí výstražného trojúhelníku. Alarm je opět možno vypnout, pomocí tlačítka, které je mu přiřazeno ve webovém rozhraní. V tomto případě zůstávají všechny čidla v režimu v jakém byli při sepnutí alarmu. Stejně je tomu i v případě, kdy je alarm vypnut prostřednictvím ústředny. Ukázka signalizace spuštěného alarmového hlášení je na následujícím obrázku.

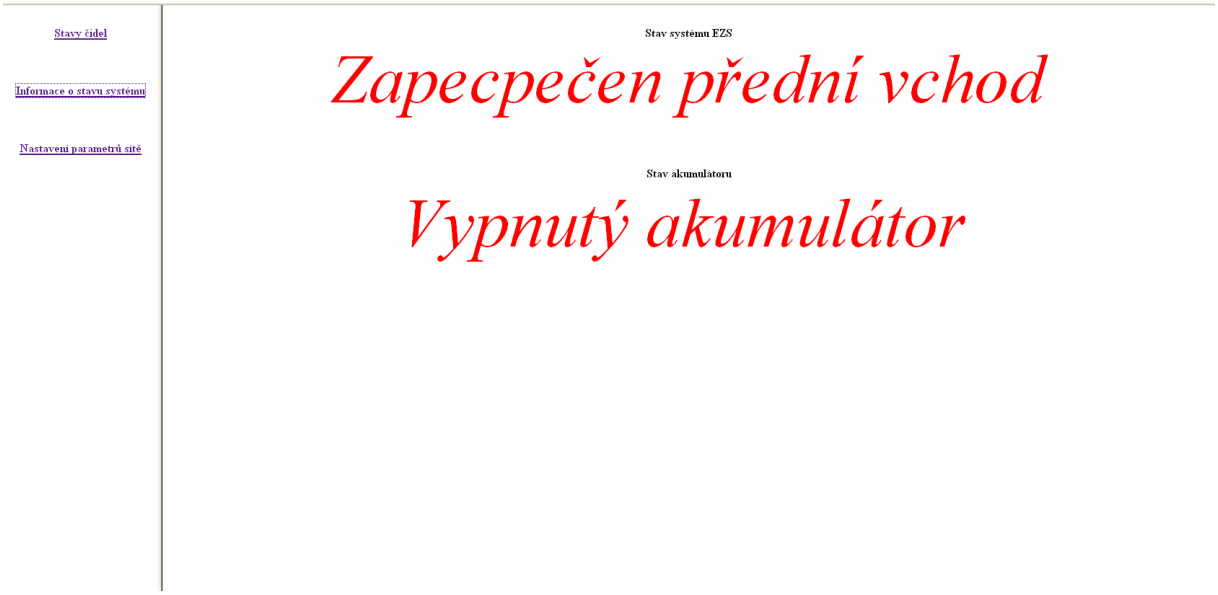


Obrázek č.10 – Alarmové hlášení

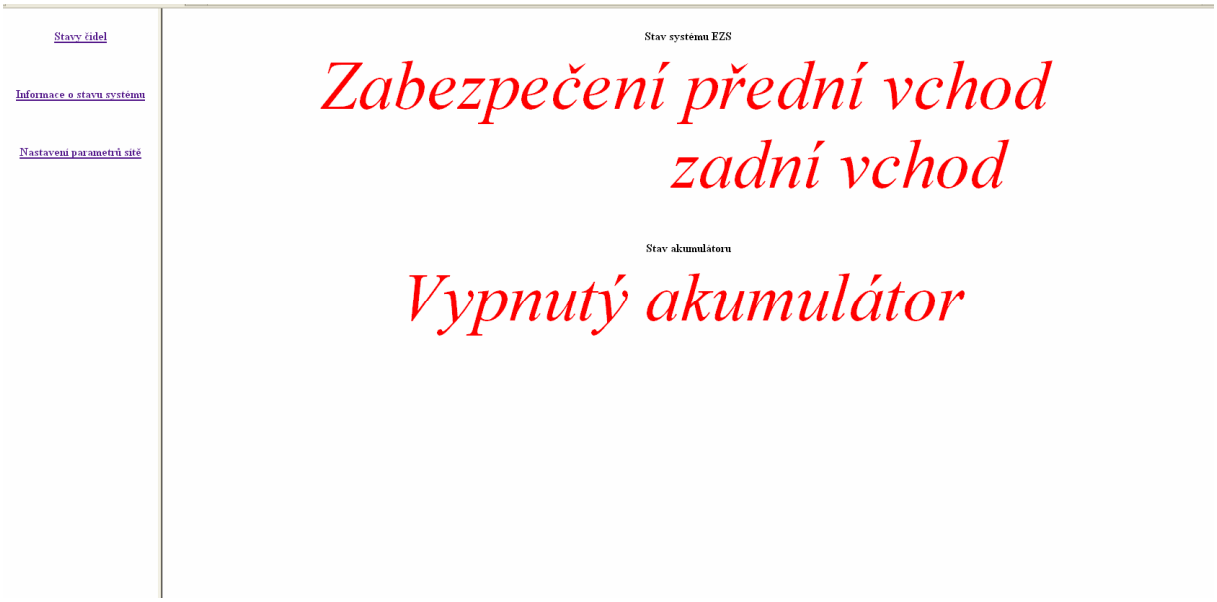
Jednotlivé stavy se po ovládání pomocí webového rozhraní aktualizují okamžitě. V případě, kdy je provedena změna ovládáním přímo na ústředně, je třeba webové rozhraní aktualizovat. Jinak se na něm provedené změny neprojevují.

5.2.2 Informační část o stavu EZS

Tato část je určena pro zjišťování celkového aktuálního stavu, ve kterém se daný monitorovaný EZS připojený na modul vzdáleného přístupu právě nachází. V mém případě budou rozlišovány dvě funkce. První z nich je zobrazení toho, která čidla jsou v jakém stavu. Detekovány jsou pouze stavy zastřežených čidel. V tuto chvíli se tedy dozvíme, jaká čidla jsou zabezpečena. V případě, že sepnuto není ani jedno čidlo je dána uživateli informace o tom, že systém je v klidu. V případě, že jsou všechna čidla v režimu střežení je zobrazeno hlášení o kompletním zabezpečení systému. Ukázky informací, které jsou webovým rozhraním uživateli poskytovány jsou zobrazeny na následujícím dvou snímcích. Tyto informace plně korespondují s informacemi, které uživatel může vidět i pomocí zobrazení pro jednotlivá čidla.



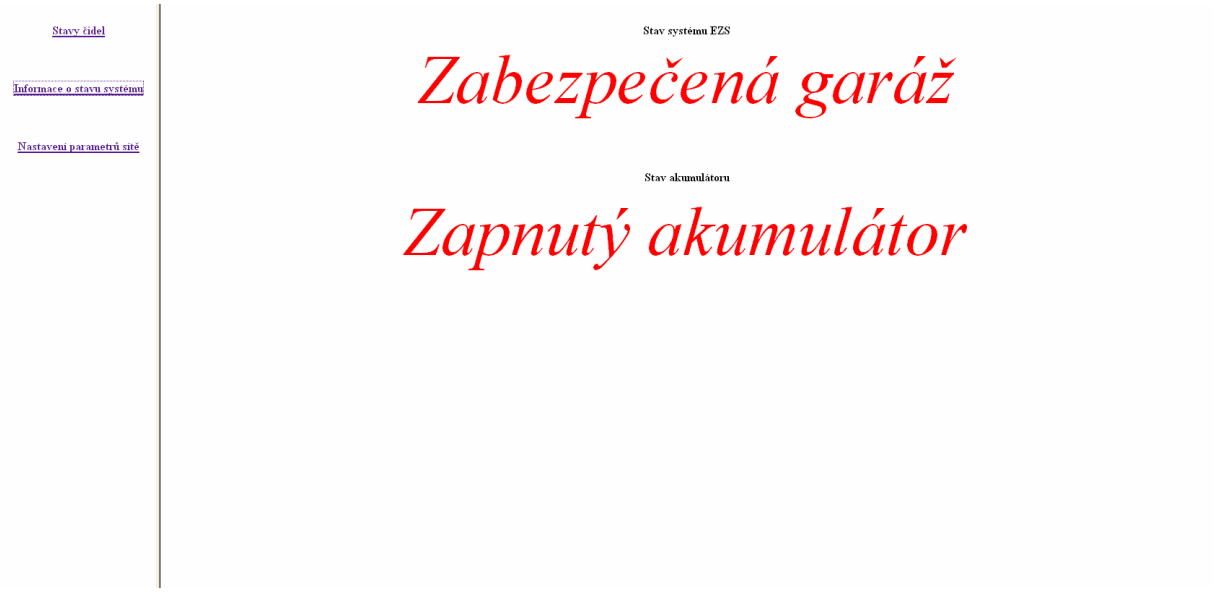
Obrázek č.11 – Ukázka informací poskytovaných uživateli



Obrázek č.12 – Ukázka informací poskytovaných uživateli

Druhou částí je informace o akumulátoru, který slouží k případnému napájení ústředny a tím i k napájení samotného EZS. V mém případě v této části nastal problém, jakým způsobem běžnou součást, která je uživateli poskytována simulovat na mnou vytvořeném webovém rozhraní. Problém je v tom, že napájení na

simulačním prostředku je prováděno ze sítě. Bylo tedy nutné najít způsob, jakým simulovat hlášení akumulátoru. Rozhodl jsem se pro velice jednoduchou možnost. Aby bylo vidět, že tato část funguje provedl jsem potenciální sepnutí akumulátoru ve chvíli, kdy je spuštěno detekování alarmu. V jiném případě tato část kódu neprobíhá a signalizace říká, že akumulátor je vypnutý. Tato část slouží opravdu pouze jako simulace této informace, aby byla na webovém rozhraní patrna její funkčnost. Zobrazení, kdy je v simulaci spuštěn akumulátor je na **Obrázku č.13.**

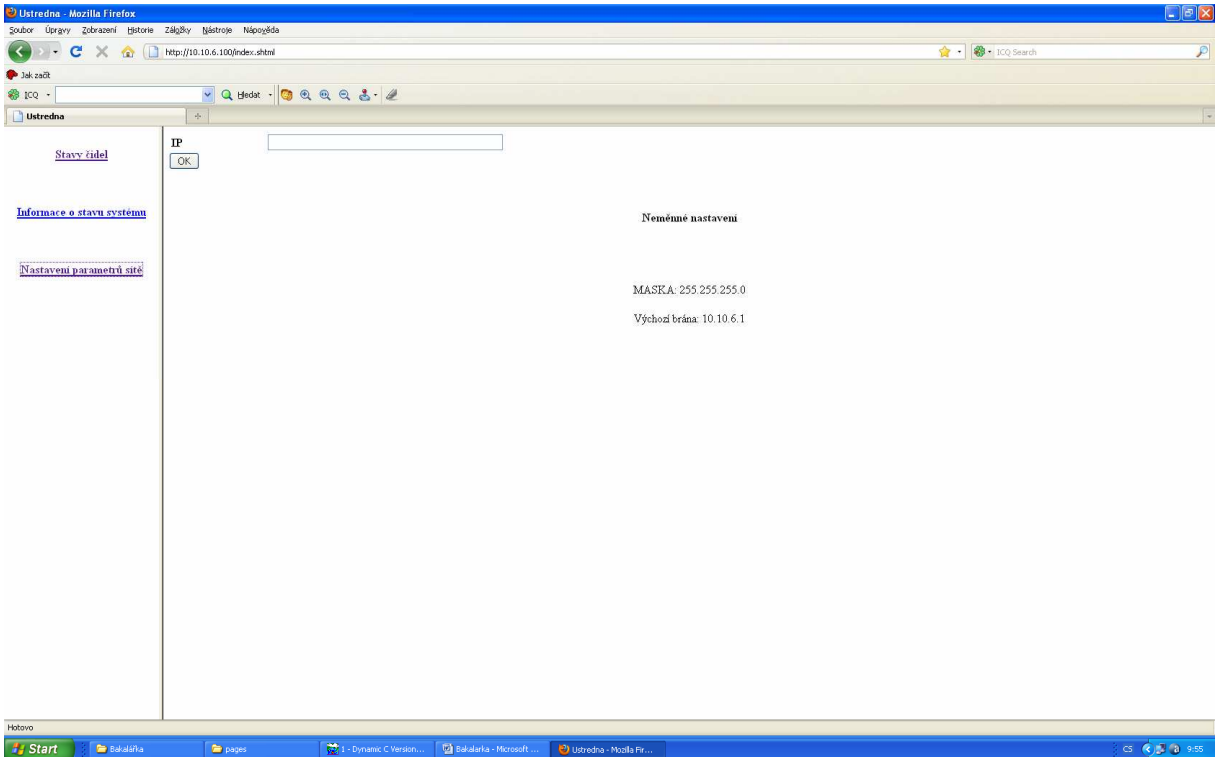


Obrázek č.13 – Spuštění akumulátoru

5.2.3 Změna parametrů sítě

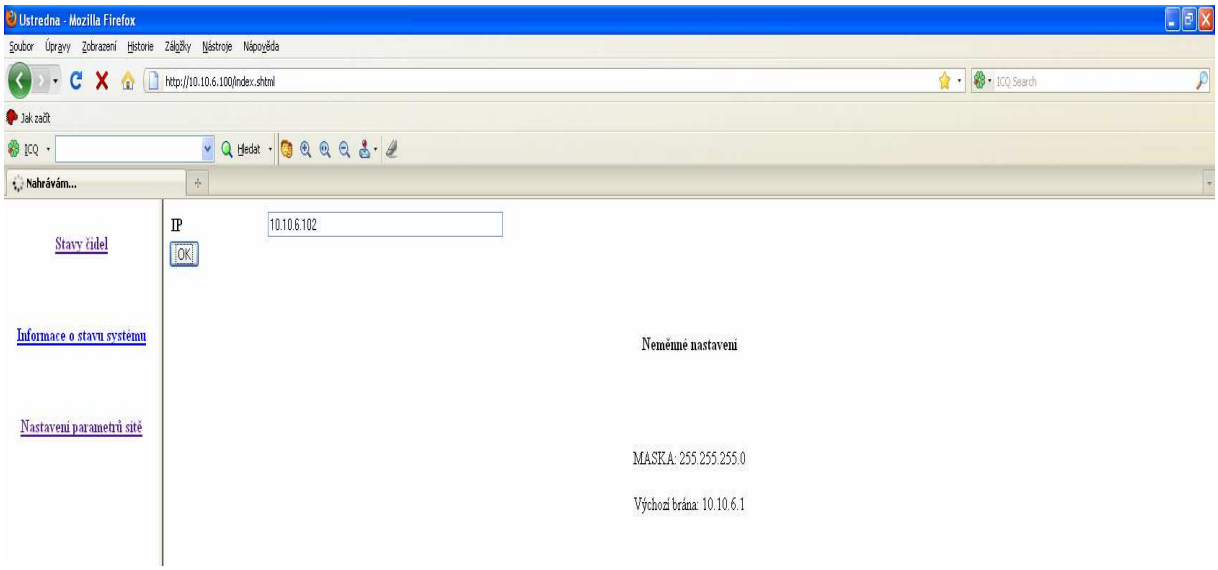
Zřejmě nejdůležitější součást webového rozhraní. Umožňuje uživateli nastavení IP adresy, podle které bude v síti rozlišen samotný modul vzdáleného přístupu. Uživatel bude mít možnost zadat si vlastní IP adresu v daném rozsahu, který je pevně stanoven. Tento rozsah je stanoven pevně od adresy, která je závislá na adresaci zvolené sítě (výchozí brány, masky podsítě a základního nastavení IP adresy). V mém případě jsou podporovány adresy 10.10.6.100 až po adresu 10.10.6.200, jako výchozí brána je použita adresa 10.10.6.1. Tato adresa je třeba nastavit v nastavení sítě jako adresu samotného PC. Maska sítě a také výchozí bránu nebude z hlediska

uživatele možno měnit. Uživatel zadává adresu v textovém formátu. Ukázka výchozího nastavení IP adresy je na následujícím snímku.



Obrázek č.14 – Původní nastavení IP adresy

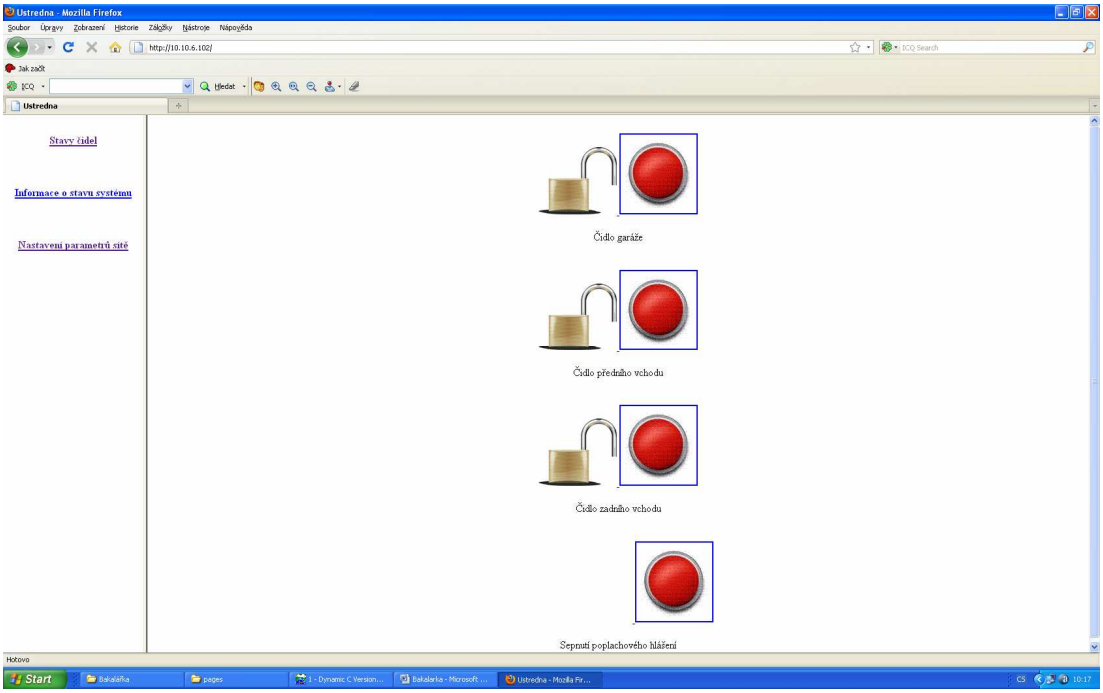
Jak je patrno z **Obrázku č.14** není přesně vidět jaká IP adresa je právě používána. Tato část, ale není v našem případě až tak nutná, protože použitá adresa je vidět při zadávání HTTP serveru a zobrazování samotné stránky. V našem případě je jako výchozí použito nastavení IP adresy 10.10.6.100 a nastavení zbylých neměnných částí je zobrazeno pod polem pro zadání IP adresy. V případě, kdy chceme změnit IP adresu je třeba zadat ji v daném rozsahu do pole v běžném tvaru v jakém je IP adresa zadávána. Po stisku tlačítka OK je adresa modulu změněna. Ukázku provedu za změně adresy ze základní na adresu 10.10.6.102. Postup provedení změny je na následujícím obrázku.



Obrázek č.15 – Změna IP adresy

V případě, kdy je IP adresa změněna není již samotné rozhraní aktualizováno a je třeba zadat správnou adresaci, tedy do pole, ve kterém je adresa webového rozhraní zadáme adresaci http://“IP“. IP označuje novou adresu, která je uvedena v poli IP, které je zobrazeno na **Obrázku č.15.** V našem případě tedy zadáme http://10.10.6.102 při tomto zadání získáme obnovené webové rozhraní, které funguje na nové IP adrese. Ukázka a důkaz jsou uvedeny níže.

Obrázek č.16 – Důkaz změny IP adresy modulu vzdáleného přístupu



Obrázek č.17 – Ukázka funkčnosti modulu se změněnou IP adresou

6. ZÁVĚR

Mým úkolem v této práci bylo provést návrh koncepce modulu vzdáleného přístupu a poté provést jeho jednoduchou formu aplikace na zvoleném vývojovém prostředku. Pro samotný návrh bylo třeba vycházet z jednotlivých norem, které jsou vztaženy na problematiku EZS. Nejdůležitější části, ze kterých bylo vycházeno jsou shrnuty v kapitolách 2 a 3.

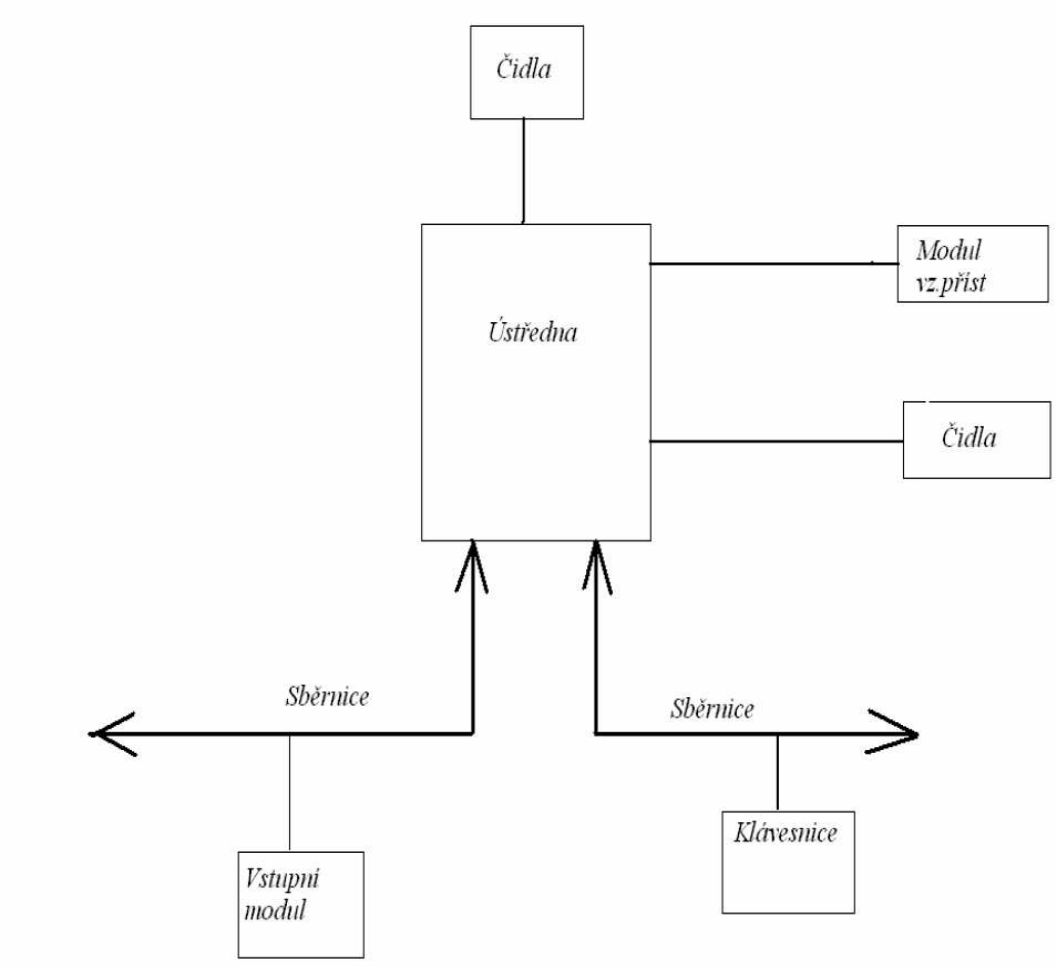
Modul je navržen pro použití ve třídách prostředí I a II a také pro stejné stupně zabezpečení,tedy stupně zabezpečení 1,2. Musí tedy splňovat dané stanovené pro tyto podmínky vztahující se k EZS. Jednotlivé vlastnosti které modul splňuje jsou shrnuty v **Tabulce č.6.**

Vlastnost	**Typ**
Stupeň zabezpečení	1,2
Třída prostředí	I,II
Úroveň přístupu	Přístup pro všechny uživatele
Doba monitorování propojení	60 sekund
Signalizace	Pomocí LED diod
Propojení modulu s ústřednou	Sériová linka
Ovládání modulu uživatelem	Rozhraní Internet
Informace získané z ústředny na modul	Stav čidel, Stav indikace,Nastavení sítě, Indikace alarmových hlášení
Možnosti pro uživatele	Sepnutí čidel, Vypnutí alarmového hlášení, Změna IP adresy v rámci nastavené sítě, Kontrola běhu akumulátoru a stavu EZS,

Tabulka č.6 – Shrnutí vlastností navrženého modulu

Pokud je to technologicky možné může být navržený modul vzdáleného přístupu použit i ve vyšších třídách zabezpečení.

Z hlediska sítě je modul konstruován tak, že je zapojován do určité známé sítě, která je nastavena při instalaci tohoto modulu samotných technikem ve spolupráci se správcem sítě, který daný modul zapojuje. Poté je umožněno uživateli volit pouze různé IP adresy,samotné přednastavení sítě provádí v mém případě správce sítě a následně technik firmy, který zapojuje EZS. Podle toho je také konstruováno samotné webové rozhraní a na simulačním příkladě umožněna podpora 100 různých IP adres. HTTP port je pro navržený modul vzdáleného přístupu pevně s stanoven jako port 80



Obrázek č.18 – Blokové schéma EZS s modulem vzdáleného přístupu

7. LITERATURA

[1] Podniková směrnice Jablotron s.r.o.,Poplachové systémy – Elektrické zabezpečovací systémy, Část 1:Všeobecné požadavky

[2] Paradox Security Systém,Manuál modulu vzdáleného přístupu IP100, verze 1.2.1

[3] Rabbit SBC Demonstration Board[online],
naposledy navštíveno 17.5.2010
URL http://www.rabbit.com/products/demo_board/index.shtml

[4] RABBIT Semiconductor, Rabbit 2000™ TCP/IP DEVELOPMENT KIT Getting Started,

SEZNAM SYMBOLŮ,VELIČIN A ZKRATEK

EZS	Elektrický zabezpečovací systém